

**Congress of the United States**  
**Washington, DC 20515**

November 5, 2021

The Honorable Gina Raimondo  
Secretary of Commerce  
U.S. Department of Commerce  
14th Street and Constitution Ave NW  
Washington, DC 20230

Secretary Raimondo,

We write to commend you on the bold, early actions of the Commerce Department in tackling the national security threats posed by digital surveillance technologies and to urge further action. Specifically, the entity listing of NSO Group and the proposed addition of cyber-intrusion tools to US export control lists reflect the dramatic threat these types of tools posed to human rights around the world. Furthermore, they signal that human rights are a guiding principle of United States policy.

The recent revelations surrounding NSO Group's Pegasus software amplified important questions for us on how sensitive and powerful technologies are used by foreign governments against Americans, as well as against journalists and civic activists. When private companies develop these sophisticated hacking tools, they should never be sold on the open market to authoritarian states. Just as we would never tolerate a company selling sensitive drone or hypersonic missile technologies to countries that might use them against Americans, we shouldn't give blank checks to companies selling hack-for-hire services. We need to establish similar non-proliferation and export rules for the cyber world, and work with our partners to hold accountable companies that violate those rules.

As such, the entity listing of NSO Group and the alignment of the United States with plurilateral controls on cyber-intrusion tools through the Wassenaar Arrangement are an important first step in countering digital surveillance regimes. However, we believe additional steps are warranted.

First, we are concerned that the entity listing of NSO Group and Candiru do not eliminate the risk that US investors remain complicit in the companies' past and ongoing exports. As your press release notes, these companies "supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers," threatening "the rules-based international order."<sup>i</sup> While the entity listing will ensure that US technology exporters cannot supply these companies, we urge you to also work to ensure that American pension funds and 401Ks are not inadvertently complicit in subsidizing these abusive business models. This could require new trade-related regulations and consideration of such companies for sanction under existing human rights regimes or a new targeted set of surveillance-related sanctions.

Second, the addition of cyber-intrusion tools to US control lists targets a very dangerous but narrow set of items that are directly linked to 21<sup>st</sup> century surveillance architectures. We are concerned by reporting that a broader set of U.S.-origin items and services have—perhaps inadvertently—been linked to digital surveillance regimes linked to gross violations of human rights. Current export regulatory structures imposed on surveillance-related goods such as surveillance network-control systems, surveillance analytic systems, or network monitoring tools have failed to comprehensively prevent U.S. companies and investors from feeding these items into surveillance architectures that directly enable grave abuses. For example, these types of US-origin items have been linked to the ethnic profiling and concentration camps in Xinjiang, China. Therefore, we urge you to consider a set of stronger measures that would assure the American people that US companies are not complicit in digital repression.

As you know, the Export Control Reform Act of 2018 gives the Department of Commerce the authority to regulate exports in order to “carry out the foreign policy of the United States, including the protection of human rights and the promotion of democracy” (50 USC 4811). Furthermore, U.S. law asserts firmly that the international defense of human rights is in the interests of the United States: “A principal goal of the foreign policy of the United States shall be to promote the increased observance of internationally recognized human rights by all countries” (22 USC 2304).<sup>ii</sup> As such, we urge you to follow up on these first steps with the following measures:

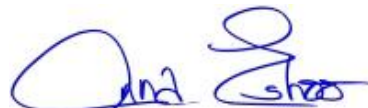
1. Consider the abusive clients of NSO Group and other such problematic companies for sanction under the Global Magnitsky Act and consider the establishment of a targeted sanctions regime to hold accountable individuals and companies that sell these tools to authoritarian states.
2. Inform investors and financial institutions of the risks related to the export of items and services with surveillance capabilities, providing demonstrative cases of exports linked to abuse.
3. With the assistance and input of civil society and the intelligence community, develop a broader list of items and services with surveillance capabilities subject to U.S. control that could be used to abuse human rights.<sup>iii</sup>
4. Propose a new rule amending the Export Administration Regulations to identify end uses and end users to which transfer of these items should require a license, including destination countries.
5. Work with the State Department to develop a regularly updated list of destination countries determined to have used items and services with surveillance capabilities in violation of basic human rights, including to silence dissent, sanction criticism, punish independent reporting (and sources for that reporting), manipulate or interfere with democratic or electoral processes, persecute minorities and vulnerable groups, or target advocates of human and democratic rights (including activists, journalists, artists, minority communities, or opposition politicians)—to serve as a basis for such an end-user license requirement.
6. Propose a rule to require provisos for any approved licenses for these newly identified surveillance items and services, drawn from recommended contract terms in the State Department’s *Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, including regular human rights due diligence reports, limitations for legitimate use, clawback terms, and duty to notify the Department if the item or service is linked to human rights abuses.
7. Work with the State Department to add these items to multilateral control regimes, including the Wassenaar Arrangement, and to cooperatively identify with international partners new surveillance technologies linked with human rights abuse.

When U.S. investors prop up companies like NSO Group, this implies the assent of the U.S. government, encouraging such companies to continue providing dangerous tools like *Pegasus* to the most repressive governments. Conversely, when the United States responsibly uses its markets and trade regulations to defend human rights, authoritarian governments take note and the international norms to which our nation is committed are strengthened. We look forward to engaging with you on these urgent requests.

Respectfully,



Tom Malinowski  
Member of Congress



Anna G. Eshoo  
Member of Congress



Katie Porter  
Member of Congress



Joaquin Castro  
Member of Congress

cc: The Honorable Antony Blinken, Secretary of State, U.S. Department of State

---

<sup>i</sup> U.S. Department of Commerce: [Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities](#) (November 3, 2021)

<sup>ii</sup> This same law further obligates the President to make security assistance policy decisions in a manner that will “avoid identification of the United States... with governments which deny to their people internationally recognized human rights and fundamental freedoms.” 22 USC 2304.

<sup>iii</sup> We recommend you start with the definition of “Product or Service with Intended or Unintended Surveillance Capabilities” in the Department of State’s [Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities](#) (September 30, 2020):

*Product or Service with Intended or Unintended Surveillance Capabilities: “product or service with intended or unintended surveillance capabilities” is defined as a product or service marketed for or that can be used (with or without the authorization of the business) to detect, monitor, intercept, collect, exploit, preserve, protect, transmit, and/or retain sensitive data, identifying information, or communications concerning individuals or groups.*